

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF
1006 BULLITT AVENUE SE, ROANOKE,
VA 24013, TO INCLUDE ALL
OUTBUILDINGS, VEHICLES AND THE
CURTILAGE SURROUNDING THE
PROPERTY

UNDER SEAL

Case No. 7:21mj157

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION TO SEARCH AND SEIZE**

I, Jason Shilling, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant to search the premises, outbuildings, and curtilage of the location known as 1006 Bullitt Avenue SE, Roanoke, VA 24013 (**Target Address 1**). **Target Address 1** is located in the City of Roanoke, Virginia, within the Western District of Virginia further described in Attachment A, for the things described in Attachment B.

2. I am a Task Force Officer with the Drug Enforcement Administration, and have been since September 2019. I have been employed by the Salem Police Department since January 2015. Prior to this DEA assignment, I spent 2 years assigned to the Salem Police Department Special Investigations Unit as a narcotics detective with the Roanoke Valley Regional Drug Unit. During these assignments, I have made narcotics arrests that have led to convictions at both the State and Federal levels. I am familiar with the methods and patterns of illegal drug trafficking at both the street and wholesale level. I have participated in the

debriefings of defendants, informants, and witnesses who had personal knowledge of major drug trafficking organizations. Additionally, I have experience with observing drug related electronic communications in defendants' cellular phone downloads and have observed drug-related communications that have been captured in law enforcement covert recording equipment. I know from my training and experience that drug dealers commonly safeguard illegal narcotics and proceeds from drug distribution inside their residences. Also, I know from my training and experience that cellular devices are used to facilitate drug trafficking. I am further aware that the memory contents of these cellular devices often contain information of significant evidentiary value.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended only to establish sufficient probable cause for the requested search warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that **Target Address 1** contains evidence of violations of distribution and possession with intent to distribute controlled substances, in violation of Title 21, United States Code, Section 841, and conspiracy to distribute controlled substances, in violation of Title 21, United States Code, Section 846. There is probable cause to search the location described in Attachment A for evidence, contraband, and/ or fruits of these crimes further described in Attachment B.

IDENTIFICATION OF THE PROPERTY TO BE SEARCHED

5. The property to be searched is as follows:
 - a. **Target Address 1** is a residence located at 1006 Bullitt Avenue SE, Roanoke, VA 24013. **Target Address 1** is described as a single family residence with grey siding and white trim. The numbers “1006” are affixed to the right of the front door as well directly above the access point to the front porch (See Attachment A). It is believed that John Luther BRUCE uses this location as his primary residence as well as a storage location for narcotics.

STATEMENT OF PROBABLE CAUSE

6. Since March 2021, the Drug Enforcement Administration (DEA) has been investigating John Luther BRUCE as a distributor of narcotics, specifically crystal methamphetamine, in the Roanoke, VA area.

7. In March 2021, DEA Investigators met with a DEA confidential source who spoke about his/her knowledge of John BRUCE’s narcotics distribution. The confidential source identified BRUCE as a methamphetamine distributor. The confidential source also stated that he/she has seen multiple pound quantities of methamphetamine at BRUCE’s residence.

8. In May 2021, the DEA conducted a controlled purchase of a quantity of methamphetamine utilizing a confidential source (CS). The CS made contact with BRUCE on a recorded phone call to initiate the transaction. John BRUCE made arrangements for the CS to meet with BRUCE’s wife, Dorothy Jane BRUCE, at their residence of 819 Highland Avenue SE, Roanoke, VA 24013. John BRUCE has since moved from this location to **Target Address 1**.

The confidential source paid Dorothy BRUCE in U.S. currency for the quantity of methamphetamine. During the deal, Dorothy BRUCE went upstairs in the residence and returned with the quantity of narcotics, indicating that distributable amounts of methamphetamine were being stored in the residence.

9. In October 2021, Virginia State Police Drug Enforcement Section conducted a controlled purchase of a quantity of methamphetamine with John Luther BRUCE as the supplier of the narcotics. Prior to the transaction, surveillance was established at 1006 Bullitt Avenue SE, Roanoke, VA 24013. John BRUCE was observed walking from the rear of the residence and entering a green Ford F-150 pickup truck bearing VA registration UEE-9796. Surveillance units followed BRUCE to the predetermined meeting location in Roanoke, VA where the confidential source paid BRUCE in U.S. currency for the quantity of methamphetamine. BRUCE was not observed making any stops between **Target Address 1** and the location of the deal which indicates the narcotics were stored in **Target Address 1**.

10. In November 2021, Virginia State Police Drug Enforcement Section conducted a second controlled purchase of a quantity of methamphetamine with John Luther BRUCE as the supplier of the narcotics. The CS spoke with John BRUCE on a recorded phone call to set up the narcotics transaction, during which BRUCE provided a location for the transaction. Prior to the transaction, surveillance units located BRUCE and a green Ford F-150 (VA Registration: UEE-9796), which was registered to John BRUCE, near the area where BRUCE advised the CS to meet. BRUCE was seen meeting with an unidentified male subject and an unidentified female subject before the CS met BRUCE at a predetermined location in Roanoke, VA and paid BRUCE with U.S. currency for the quantity of methamphetamine.

11. During the past 72 hours, your affiant has conducted surveillance at **Target Address 1**. During surveillance, John BRUCE has been seen entering/ exiting the residence. Additionally, BRUCE's green Ford F-150 (VA Registration: UEE-9796) has been seen parked behind **Target Address 1**.

12. Based upon my training, expertise, and experience, I know that:

- a. Distributors of controlled substances and money launderers often keep ledger books, telephone books, receipts, drug/money customer lists, photographs and other papers that identify co-conspirators and their locations or residences and that relate to the importation, transportation, purchasing and distribution of controlled substances and proceeds derived from said sales;
- b. Drug traffickers generate substantial profits because of drug dealing which the courts have recognized as probative evidence of crimes motivated by greed, in particular, trafficking controlled substances. Drug traffickers often place assets in corporate entities in order to avoid detection of those assets by law enforcement agencies. These assets often are placed in other person's names, even though the drug dealers continue to use these assets and exercise dominion and control over them. They also often maintain on hand large amounts of United States currency in order to operate and finance their ongoing drug business;
- c. Drug traffickers commonly "front" (i.e. provide on consignment) controlled substances to their clients and the aforementioned books, records, receipts, notes, ledgers, etc. are maintained where the drug traffickers have ready access to them. It is common practice for large-scale drug dealers to conceal contraband, proceeds

and drug sales and records of drug transactions in secure locations within their residences, stash houses, and/or places of business for ready access and to conceal such items from law enforcement authorities. Persons involved in large scale drug trafficking often conceal in their residences, stash houses, and/or places of business, caches of drugs, large amounts of currency, financial instruments, precious metals, jewelry, automobile titles and other items of value which are proceeds of drug transactions and evidence of financial transactions relating to obtaining, transferring, secreting or spending large sums of money acquired from engaging in narcotics trafficking activities;

- d. When drug traffickers amass large proceeds from the sale of drugs, they often attempt to legitimize or “launder” these profits. To accomplish this, drug traffickers may utilize, but are not limited to, domestic and foreign banks and/or financial institutions and their attendant services, such as securities, cashier’s checks and money drafts;
- e. It is common practice for large-scale drug traffickers to travel to their source and distribution points to facilitate their trafficking. After purchasing their drugs, drug traffickers often transport or cause to be transported their drugs to areas in which they will distribute them. The methods of transportation include, but are not limited to, commercial carriers, private airplanes, ocean going motor vessels, rental or private automobiles, and government or contract mail carriers;
- f. Drug traffickers commonly cause to be taken photographs of themselves, their associates, their property and items used in the distribution of controlled

substances. These traffickers usually maintain these photographs at their residences or places of business;

- g. Narcotics traffickers use safes, surreptitious compartments and money counting machines to count and store the profits of their narcotics business;
 - h. Narcotics traffickers commonly possess at their residences, stash houses, or places of business, drugs, paraphernalia, and materials for packaging, cutting, weighing and distributing heroin, including, but not limited to scales, plastic wrap, plastic baggies, paper slips, tin foil, stamp pads, stamp ink and various cutting agents;
 - i. Drug traffickers commonly use electronic devices and storage components including, but not limited to, cellular telephones, computers, telex machines, facsimile machines, currency counting machines, telephone answering machines, computer software, tapes, discs, CD, DVDs, and audio tapes to store records of drug sales, ledgers, supplier's/customer's contact information, financial records, images, audio/video recordings and other related documents related to the trafficking and sale of narcotics;
13. Based on the aforementioned, your affiant respectfully submits that there is probable cause to believe that U.S. currency, documentation, and/ or other items related to the illegal distribution of narcotics further described in Attachment B will be located in **Target Address 1**.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

14. As described above and in Attachment B, this application seeks permission to search for records that might be found at **Target Address 1**, in whatever form they are found.

One form the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41 (e)(2)(B).

15. *Probable Cause.* I submit that if a computer or storage medium is found at the **Target Address 1**, there is probable cause to believe relevant records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer

has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

16. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on any storage medium in **Target Address 1** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other

external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the Criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the

computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the Crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a Crime (e.g., internet searches indicating Criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw

conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

17. *Necessity of seizing or copying the entire computers or storage media.* In most cases, a thorough search of a premise for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

18. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it contains evidence described by the warrant.

CONCLUSION

19. I submit that this affidavit supports probable cause for a search warrant of the properties described in Attachment A, in order to seek the items described in Attachment B.

Respectfully Submitted,

S/ Jason Shilling
Jason Shilling
Task Force Officer
Drug Enforcement Administration

Subscribed and sworn by telephone on November 19, 2021.

Robert S. Ballou
UNITED STATES MAGISTRATE JUDGE